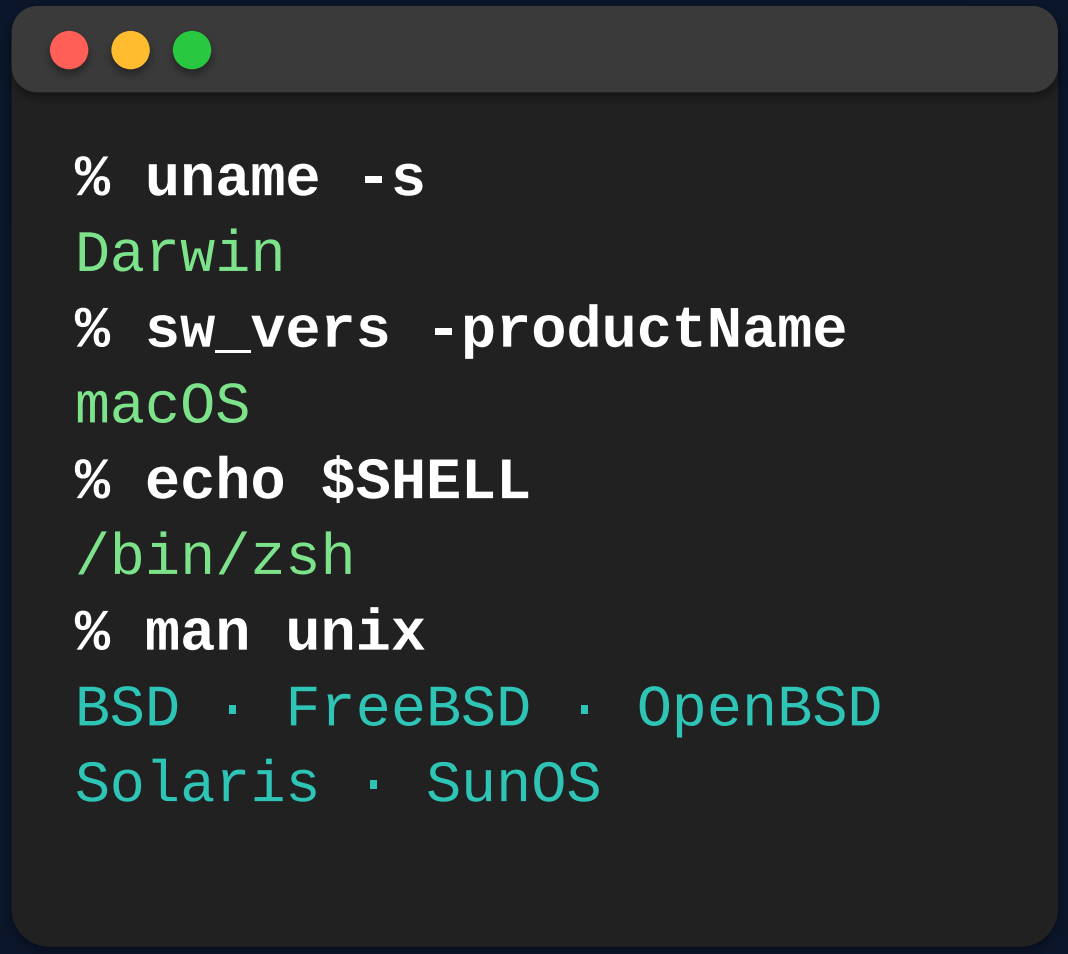


LESSON 11 OF 12

macOS UNIX

Darwin & BSD

Storage, APFS, Security & Backup

Full Course · macOS 27 Golden Gate

What You Will Learn in Lesson 11

- APFS: containers, volumes, snapshots and clones
- diskutil: list, inspect, add volumes, erase, verify
- Disk images with hdiutil, including encrypted ones
- Security layers: FileVault, SIP, Gatekeeper, TCC, XProtect
- ACLs, extended attributes, quarantine and file flags
- Time Machine and tmutil; the 3-2-1 backup rule
- ZFS and encryption on FreeBSD, OpenBSD and Solaris

APFS in One Slide

Concept	What it means
Container	A pool of space on one disk partition; volumes inside share it
Volume	A file system: Macintosh HD (System), Data, Preboot, Recovery, VM
Volume group	System + Data volumes that appear as one tree (firmlinks)
Snapshot	A read-only, point-in-time copy; Time Machine and updates use them
Clone	cp -c copies a file instantly; space is used only for changes
Encryption	Built in; FileVault encrypts the Data volume

diskutil: See and Manage Disks

```
% diskutil list                          # every disk, container, volume
% diskutil info / | grep -E 'Volume Name|File System|FileVault|Free'
% diskutil apfs list | less              # containers in detail

% sudo diskutil apfs addVolume disk3 APFS Projects   # shares the space
% diskutil apfs deleteVolume /Volumes/Projects
% diskutil verifyVolume /                # check (First Aid, read-only)
% diskutil apfs listSnapshots /
% df -h /;  du -sh ~/* | sort -h | tail # space used, biggest folders
```

Container names (disk3) vary: read them from diskutil list first.

External Disks: Format, Mount, Eject

```
% diskutil list external                          # find the USB disk, e.g. disk4
% diskutil eraseDisk APFS MyUSB GPT disk4         # Mac only (ERASES disk4!)
% diskutil eraseDisk ExFAT SHARE GPT disk4        # Mac + Windows + Linux

% diskutil unmount /Volumes/MyUSB;  diskutil mount MyUSB
% diskutil eject disk4

# Formats macOS reads/writes: APFS, Mac OS Extended (HFS+), ExFAT, MS-DOS (FAT32)
# NTFS: read-only by default
```

Triple-check the disk identifier before any erase command.

Disk Images: hdiutil

```
% hdiutil create -size 2g -fs APFS -volname Vault \
      -encryption AES-256 -stdinpass ~/vault.dmg      # type a password
% hdiutil attach ~/vault.dmg                          # asks for it
% cp ~/lab/*.sql /Volumes/Vault/
% hdiutil detach /Volumes/Vault

% hdiutil create -srcfolder ~/lab -format UDZO ~/lab.dmg   # compressed copy
% hdiutil verify ~/lab.dmg
% cp -c bigfile.iso clone.iso      # APFS clone: instant, no extra space
```

The Security Layers of macOS

Layer	Protects	Check it
FileVault	Data at rest if the Mac is stolen	fdesetup status
System Integrity Protection	System files, even from root	csrutil status
Signed System Volume	The OS itself, by a cryptographic seal	diskutil info / | grep -i sealed
Gatekeeper + notarization	Against untrusted apps	spctl --status
TCC privacy controls	Camera, mic, files, Full Disk Access	System Settings → Privacy & Security
XProtect	Known malware, updated by Apple	automatic

FileVault, SIP and Gatekeeper From Terminal

```
% fdesetup status
FileVault is On.
% sudo fdesetup enable                    # prints a recovery key: store it safely!
% sudo fdesetup list                      # users who can unlock the disk

% csrutil status
System Integrity Protection status: enabled.

% spctl --status                          # assessments enabled
% spctl -a -vv /Applications/Safari.app   # accepted? who signed it?
% tccutil reset Camera                    # reset camera permissions
```

ACLs, Extended Attributes and Flags

```
% chmod +a "labstudents allow read,write" ~/Shared-Lab      # add an ACL entry
% ls -le ~/Shared-Lab                      # show ACLs (the + sign)
% chmod -a# 0 ~/Shared-Lab                 # remove entry 0;  chmod -N removes all

% xattr -l ~/Downloads/tool.zip            # extended attributes
com.apple.quarantine: 0083;...;Safari;...
% xattr -d com.apple.quarantine ~/Downloads/tool.zip   # only if you trust it!

% chflags uchg important.txt;  ls -lO important.txt     # immutable flag
% chflags nouchg important.txt
```

Time Machine and tmutil

```
# GUI: System Settings → General → Time Machine → Add Backup Disk
% sudo tmutil setdestination -a /Volumes/TM-Backup
% tmutil destinationinfo
% tmutil startbackup --block            # back up now and wait
% tmutil latestbackup;  tmutil listbackups | tail -3
% sudo tmutil addexclusion -p ~/Downloads   # skip a folder
% tmutil localsnapshot;  tmutil listlocalsnapshots /

# Restore one file: open its folder → Enter Time Machine, or:
% tmutil restore <backup-path>/Users/wahid/lab/school.db ~/lab/
```

The 3-2-1 Backup Rule

- 3 copies of your data: the original + 2 backups
- 2 different kinds of storage (e.g. external SSD + network/cloud)
- 1 copy off-site (another building or the cloud)
- Automate it: Time Machine, launchd + rsync, database dumps
- Encrypt backups that leave your control
- Test a restore every month — an untested backup is only a hope

Storage and Security on Other UNIX Systems

	FreeBSD	OpenBSD	Solaris 11.4
Main file systems	ZFS, UFS	FFS	ZFS
Snapshots	zfs snapshot pool/home@now	(none in FFS)	zfs snapshot rpool/export/home@now
Disk encryption	GELI, ZFS native encryption	softraid CRYPTO (bioctl)	ZFS encryption
Send backups	zfs send | ssh host zfs recv	dump / restore, rsync	zfs send | zfs recv
Extra hardening	securelevel, jails, Capsicum	pledge, unveil, W^X	RBAC, zones, immutable zones

Lab: Protect the Data

```
% diskutil list;  diskutil info / | grep -iE 'sealed|FileVault'
% sudo diskutil apfs addVolume disk3 APFS Projects;  df -h /Volumes/Projects
% hdiutil create -size 200m -fs APFS -volname Vault -encryption AES-256 -stdinpass ~/vault.dmg
% hdiutil attach ~/vault.dmg && cp ~/lab/school.db /Volumes/Vault/ && hdiutil detach /Volumes/Vault
% fdesetup status;  csrutil status;  spctl --status
% mkdir ~/Shared-Lab && chmod +a "staff allow read" ~/Shared-Lab && ls -le ~ | grep Shared
% tmutil localsnapshot && tmutil listlocalsnapshots /
% diskutil apfs deleteVolume /Volumes/Projects
```

Summary & Homework

- APFS: containers share space; snapshots, clones, built-in encryption
- diskutil list / info / addVolume / eraseDisk; hdiutil for disk images
- FileVault, SIP, sealed system, Gatekeeper, TCC, XProtect
- ACLs (chmod +a), xattr quarantine, chflags uchg
- Time Machine + tmutil; follow 3-2-1 and test restores
- Next: Lesson 12 — Administering macOS: Desktop vs Server

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.